

[| NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

NASA Procedural Requirements

COMPLIANCE IS MANDATORY**NPR 1620.2A**Effective Date: October 07,
2015Expiration Date: October 07,
2020[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: Facility Security Assessments**Responsible Office: Office of Protective Services**[| TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [AppendixA](#) | [AppendixB](#) | [ALL](#) |

Chapter 1: Determining the Center/Facility Security Level

1.1 General

1.1.1. The initial FSL determination for new leased or owned space will be made as soon as practical after the identification of a space requirement (including succeeding leases). The determination should be made early enough in the space acquisition process to allow for the implementation of required countermeasures (or reconsideration of the acquisition caused by an inability to meet minimum physical security requirements.)

1.1.2 Upon the effective date of this NPR, all NASA facilities/buildings will be initially assessed using this methodology. Once the initial assessments are completed, risk assessments will be conducted at least every five years for level one and level two facilities and every three years for levels three and four facilities from the facility's previous assessment date. There will be an FSL designated for the Center overall, and each facility within the Center will have its own FSL designation. Center Chiefs of Protective Services, at their discretion, may decline to conduct assessments of buildings determined not to have any Center operational or mission support value (e.g., abandoned or decommissioned facilities, vacant sheds, and vacant trailers.)

1.1.3 Implementation of countermeasures inclusive of policies and procedures will be based on risk with the appropriate FSL level. The FSL will be reviewed and adjusted, if necessary, as part of each initial and recurring risk assessment. The responsibility for making the final FSL determination rests with the Center Director as the Designated Official (DO), who must either accept the risk or fund security measures to reduce the risk. Artificially lowering the FSL level to avoid countermeasure implementation is not permitted.

a. For single-tenant Government-owned or leased facilities, a representative of the Center's Office of Protective Services will make the FSL determination, in consultation with the Center Director responsible for the facility. For single tenant facilities owned or leased through General Services Administration (GSA), the FSL determination will be made by the Federal Protective Services in coordination with the Center Office of Protective Services and in consultation with the Center Director.

b. In multitenant Government-owned or leased facilities, the DO in coordination with a representative of each Federal tenant i.e., the Facility Security committee will make the FSL determination in consultation with the owning/leasing department or agency and the security organization(s) responsible for the facility.

c. A campus or NASA Center consists of two or more Federal facilities located contiguous to one another and sharing some aspects of the environment (e.g., parking, courtyards, vehicle access roads, or gates) or security features (e.g., a perimeter fence, guard force, or onsite central alarm/closed circuit television monitoring station). In multitenant Centers, all individual facilities in the campus will be assigned an FSL in accordance with this NPR. d. While the incorporation of additional factors and criteria makes this NPR more useful to determine the FSL for special-use and other unique facilities, such as high-security laboratories, hospitals, or unique storage facilities for chemicals or munitions, some facilities may still not fit neatly into the criteria defined here. The criticality of the mission or the symbolic nature of the facility could be such that it merits a degree of protection above that specified for a FSL Level IV facility, even though the other contributing factors, such as population or square footage may be scored lower.

(1) For example, a research laboratory might receive lower score values for symbolism, square footage, and

population size. However, the laboratory may be responsible for critical research and diagnostic activities that are vital to protecting NASA research and intellectual property that if compromised could pose a threat to the United States National Security. This mission, combined with the fact that it may be the only such laboratory in the country, would suggest that the criticality factor would far outweigh lower score values in symbolism, population, and/or facility size, and thus the facility should be considered for a Level V designation. As a result, the criteria and decision-making authority for identifying Level V facilities are within the purview of the individual Center. As general guidance, Centers should consider a facility as potentially suitable for a Level V designation if it receives a "very high" score value for criticality or symbolism and is a one-of-a-kind facility (or nearly so).

1.2 Purpose of a Center/Facility Security Level Determination

1.2.1. Not all NASA assets at all Centers and locations require the same degree of protection.

1.2.2. Protection of assets must be based on a realistic assessment of the risk associated with the types of threats likely to be directed at the assets in their actual locations, the vulnerability of the asset, the asset value, and response capabilities of law enforcement and/or security forces.

1.2.3. Performing the Center/FSL assessment allows NASA managers to establish asset protection programs appropriate for their value and the likelihood of an attempt to compromise them.

1.2.4. The Center/FSL Determination allows Center management to prioritize assets so that physical security resources can be applied in the most efficient and cost-effective manner possible.

1.3 Risk

For the purposes of this NPR, risk is the identification of credible threats, vulnerabilities, and measuring the probability of the consequences using counter-measures to mitigate the threats and vulnerabilities, and/or accepting the risk as they are associated with NASA assets.

1.4. Undesirable Events

The undesirable events to NASA facilities from criminal elements must also be evaluated in determining the FSL. Consideration must be given to the risk from more common criminal acts, such as theft, assault, unlawful demonstrations, workplace violence, and vandalism acts which historically occur more frequently at Federal facilities than acts of terrorism. Although terrorism is of concern based on past events, it should not be the default threat unless there is credible threat intelligence directly related to NASA assets. Possible sources of references could be local Center incident reports; local police reports; NASA OPS counterintelligence; and other Federal, state, and local law enforcement credible information.

1.5 Vulnerabilities

Vulnerabilities for purposes of this NPR are identified as the unmitigated threats and/or mitigated threats of a NASA asset that can be compromised. Although the vulnerability may be already mitigated, outdated technologies or more sophisticated threats may create the vulnerability.

1.6 Consequences

After identifying the threats and vulnerabilities of NASA assets, a consequence will be identified as a result of the attack. Based on the severity of the attack and the criticality of the asset, the consequence will need to be mitigated. Although the consequence could be severe, the likelihood of a threat event taking place could be low. This should not be reason to eliminate or not address the consequences of the threat and vulnerabilities. It should be a consideration of the mitigation strategy implemented.

1.7 Assets

NASA assets are people, property, and information. Much of the direction of the NASA Critical Infrastructure Protection Program (NCIPP) is directed at protecting NASA critical infrastructure assets. Typically, it is the potential publicity that would come with bombing a NASA facility or destroying and compromising a critical or symbolic NASA resource that an aggressor would find desirable. The NASA Security program is based upon protecting the greater installation, its critical facilities, and other critical assets, which will in turn provide greater protection for NASA assets.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [AppendixA](#) | [AppendixB](#)
| [ALL](#) |

| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
